--11. A method for controlling access by a requestor (7) to resources (2d) in a distributed computer system (1) comprising defining conditions for obtaining a right to a resource (2d), assigning to the requester (7) at least one role based on an access control list, defining a part of a set of resources (2d) that is accessible by a given role by a validity domain, and utilizing the validity domain of the given role to restrict the resources accessible for the given role to only part of the resources.

12. A method according to claim 11, further comprising storing an additional piece of information relative to the need to consult the validity domain of the role in the access control list.

13. A method according to claim 12, further comprising consulting the additional information relative to the need to consult the validity domain of the role and verifying that the resource in question belongs to the validity domain only if required by said information.

14. A method according to claim 12, further comprising performing an access check on two levels:

- a first-level check on the type of the resource (2d); and
- a second-level check on the identifier of the resource (2d).

15. A method according to claim 14, wherein the first-level check verifies the existence of at least one entry of the access control list that satisfies conditions for obtaining a requested right of entry, and, if the right of entry exists, the existence of a validity domain for said entry.

16. A method according to claim 15, wherein the second-level check verifies, if a requested permission for right of entry contains a resource identifier, the existence of at least one configured permission corresponding to the requested permission and the value of the additional information relative to the need to consult the validity domain.

17. A method according to claim 11, further comprising grouping rights or resources into generic groups represented by special characters or keywords or other symbols.

18. A method according to claim 12, further comprising grouping rights or resources into generic groups represented by special characters or keywords or other symbols.

19. A method according to claim 13, further comprising grouping rights or resources into generic groups represented by special characters or keywords or other symbols.

B2 cont'd

20. A method according to claim 14, further comprising grouping rights or resources into generic groups represented by special characters or keywords or other symbols.

21. A method according to claim 15, further comprising grouping rights or resources into generic groups represented by special characters or keywords or other symbols.

22. A device for controlling access by a requestor (7) to interrogated resources (2d) in a distributed computer system (1), comprising at least one management machine (2a) (2b) (2c) (2d) organized into one or more networks (3), said machine having at least one calling entity (4), for designating actions executed by the requestor (7), an application program interface (5) for transmitting interrogations from the calling entity, an access control service (6) for receiving said interrogations and controlling access of the requestors (7) to the interrogated resources (2d), storage means (10) (12) for storing roles, access control lists and validity domains and means (9) (11) (13) for accessing the storage means.

23. A device for controlling access by a requestor (7) to interrogated resources (2d) in a distributed computer system (1), according to claim 22, further comprising means for defining conditions for obtaining a right to a resource, means for assigning to the requestor at least one role based on an access control list, and

means for restricting the resources accessible for a given role to only part of the resources by means of a validity domain of the role.

24. A device for controlling access by a requestor (7) to interrogated resources (2d) in a computer system (1), according to claim 23, wherein the means for storing stores an additional piece of information relative to the need to consult the validity domain of the role in the access control list.

25. A device for controlling access by a requestor (7) to interrogated resources (2d) in a computer system (1), according to claim 24, further comprising means for consulting the additional information relative to the need to consult the validity domain of the role and verifying that the resource in question belongs to the validity domain only if required by said information.

26. A device for controlling access by a requestor (7) to interrogated resources (2d) in a computer system (1), according to claim 25, further comprising means for performing an access check on two levels:

- a first-level check on the type of the resource (2d); and
- a second-level check on the identifier of the resource (2d).

27. A device for controlling access by a requestor (7) to interrogated resources (2d) in a computer system (1), according to claim 26, wherein a first-level check verifies the existence of at least one entry of the access control list that satisfies conditions for obtaining a requested right of entry to a resource, and, if the entry exists, the existence of a validity domain for said entry.

28. A device for controlling access by a requestor (7) to interrogated resources (2d) in a computer system (1), according to claim 27, wherein a second-level check verifies if a requested right of entry to a resource contains a resource identifier, the existence of at least one configured permission corresponding to the requested right of entry and the value of additional information relative to the need to consult the validity domain.

29. A software module for controlling access by a requestor (7) to resources (2d) of a computer system comprising means for defining conditions for obtaining a right of entry to a resource (2d), means for assigning to the requestor at least one role based on an access control list, means for defining a part of a set of resources (2d) that is accessible by a given role by a validity domain, and means for utilizing the validity domain of the given role to restrict the resources accessible for a given role to only part of the resources by means of a validity domain.

30. A software module for controlling access to resources according to claim 29, further comprising means for storing an additional piece of information relative to a need to consult the validity domain of the role in the access control list.

B2 cncl

31. A software module for controlling access to resources according to claim 30, further comprising means for consulting the additional information relative to the need to consult the validity domain of the role and verifying that the resource in question belongs to the validity domain only if required by said information.

32. A software module for controlling access to resources according to claim 31, further comprising means for performing an access check on two levels:

- a first-level check on the type of the resource (2d); and
- a second-level check on the identifier of the resource (2d).

33. A software module for controlling access to resources according to claim 32 wherein the first-level check verifies the existence of at least one entry of the access control list that satisfies conditions for obtaining the requested right of entry, and, if the entry exists, the existence of a validity domain for said entry.

34. A software module for controlling access to resources according to claim 33 wherein the second-level check verifies, if the requested permission contains a resource identifier, the existence of at least one configured permission corresponding to the requested right of entry and the value of additional information relative to the need to consult the validity domain.--